

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-077274

(43)Date of publication of application : 15.03.2002

(51)Int.Cl.

H04L 12/66

H04L 12/28

H04L 29/06

(21)Application number : 2000-263873

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 31.08.2000

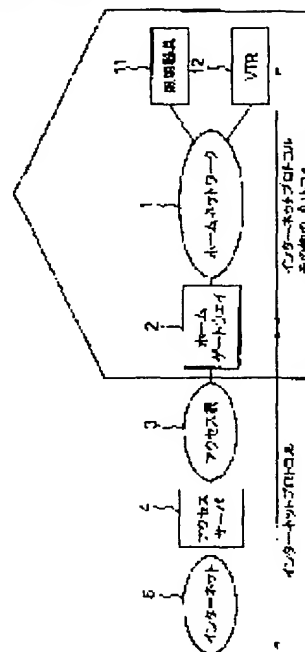
(72)Inventor : SAITO TAKESHI

## (54) HOME GATEWAY DEVICE, ACCESS SERVER AND COMMUNICATION METHOD

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a communications system, capable of preventing an attack from a hostile user to a home network, without having to provide excessive security functions to a home gateway or requiring a special management of a user.

**SOLUTION:** In order to access a VTR 12 on a home network 1 via the Internet 5 from a mobile terminal, an access number corresponding to a home gateway 2 is specified, and a message is transmitted to an access server 4; the access server 4 authenticates the mobile terminal by a predetermined method and when the authentication is confirmed, the message is transmitted to the home gateway 2 provided in the home network 1 corresponding to the specified access number via an access network 3; and the home gateway 2 receiving the message from the access server 4 which has previously been registered transmits the message to the VTR 12 via the home network 1.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-77274

(P2002-77274A)

(43) 公開日 平成14年3月15日 (2002.3.15)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テームコード* (参考)
H 0 4 L	12/66	H 0 4 L 11/20	B 5 K 0 3 0
	12/28	11/00	3 1 0 Z 5 K 0 3 3
	29/06	13/00	3 0 5 B 5 K 0 3 4

審査請求 未請求 請求項の数21 O L (全 14 頁)

(21) 出願番号 特願2000-263873 (P2000-263873)

(22) 出願日 平成12年8月31日 (2000.8.31)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 齊藤 健

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5K030 GA15 HA06 HC01 HC14 HD03

HD06 JA07 JA11 KA04

5K033 AA08 BA01 CB02 CB08 DA01

DA06 DB12 DB16

5K034 AA05 FF01 HH01 HH16 HH17

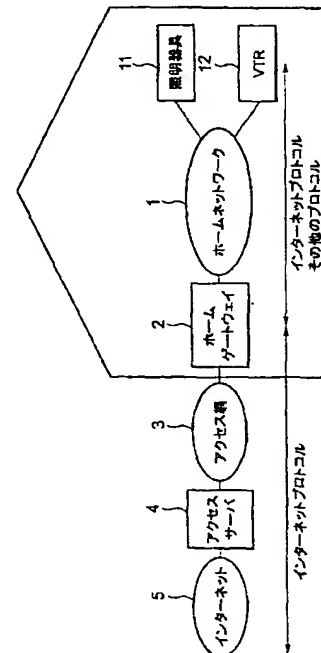
HH26 HH63

(54) 【発明の名称】 ホームゲートウェイ装置、アクセスサーバ装置及び通信方法

(57) 【要約】

【課題】 ホームゲートウェイに過度なセキュリティ機能を実装したり、そのユーザに専門的な管理を要求したりすることなしに、ホームネットワークに対する悪意ユーザからの攻撃を防ぐことを可能とする通信システムを提供すること。

【解決手段】 携帯端末からインターネット5を介しホームネットワーク1上のVTR12にアクセスするためにホームゲートウェイ2に対応するアクセス番号を指定してアクセスサーバ4へメッセージを送信し、アクセスサーバ4は携帯端末との間で該携帯端末について予め定められた方法で認証手続きを行い認証に成功した場合に指定されたアクセス番号に対応するホームネットワーク1に設置されたホームゲートウェイ2へアクセス網3を介してメッセージを転送し、予め登録されたアクセスサーバ4からメッセージを受信したホームゲートウェイ2はホームネットワーク1を介してVTR12へメッセージを転送する。



## 【特許請求の範囲】

【請求項 1】ホームネットワークの外部に位置する第 1 の通信装置から該ホームネットワーク上の第 2 の通信装置にアクセスするために、該第 1 の通信装置から、該ホームネットワークに設置されたホームゲートウェイ装置に対応するアクセス番号を指定して、該ホームゲートウェイ装置に対応するアクセスサーバ装置へ、所定のメッセージを送信し、

前記所定のメッセージを受信した前記アクセスサーバ装置は、前記第 1 の通信装置との間で、該第 1 の通信装置について、予め定められた認証方法に従って認証手続きを行い、

前記アクセスサーバ装置は、前記認証に成功した場合に、指定された前記アクセス番号に対応するホームネットワークに設置されたホームゲートウェイ装置へ、所定のアクセス網を介して、該所定のメッセージを転送し、予め登録された前記アクセスサーバ装置から前記所定のメッセージを受信した前記ホームゲートウェイ装置は、該所定のメッセージを、前記第 2 の通信装置がサポートするプロトコルに変換した上で、該ホームネットワークを介して、前記第 2 の通信装置へ転送することを特徴とする通信方法。

【請求項 2】前記ホームゲートウェイ装置は、前記所定のメッセージを前記第 2 の通信装置に転送した後に該第 2 の通信装置から情報を受信した場合には、該情報を、プロトコル変換した上で、前記アクセスサーバ装置を経由して、前記第 1 の通信装置に転送することを特徴とする請求項 1 に記載の通信方法。

【請求項 3】ホームネットワークの外部に位置する通信装置から該ホームネットワークにアクセスするために、該通信装置から、該ホームネットワークに設置されたホームゲートウェイ装置に対応するアクセス番号を指定して、該ホームゲートウェイ装置に対応するアクセスサーバ装置へ、所定のメッセージを送信し、

前記所定のメッセージを受信した前記アクセスサーバ装置は、前記通信装置との間で、該通信装置について、予め定められた認証方法に従って認証手続きを行い、

前記アクセスサーバ装置は、前記認証に成功した場合に、指定された前記アクセス番号に対応するホームネットワークに設置されたホームゲートウェイ装置へ、所定のアクセス網を介して、該所定のメッセージを転送し、予め登録された前記アクセスサーバ装置から前記所定のメッセージを受信した前記ホームゲートウェイ装置は、該所定のメッセージに基づいて選択された該ホームネットワークに係る情報を含むホームページを、前記アクセスサーバ装置を経由して、前記通信装置に転送することを特徴とする通信方法。

【請求項 4】登録されたホームネットワークのホームゲートウェイ装置に対するアクセス制御を行うアクセスサーバ装置であって、

自装置がアクセス制御を行う対象とする前記ホームゲートウェイ装置にアクセスするために使用すべき第 1 のアクセス番号と、該ホームゲートウェイ装置の設置されるホームネットワークの外部に位置する第 1 の通信装置が該ホームゲートウェイ装置または該ホームネットワーク上の第 2 の通信装置に所定のメッセージを送信する際に自装置へアクセスするために使用すべき第 2 のアクセス番号と、自装置が該第 1 の通信装置との間で行うべき認証方法とを対応付けて登録した認証テーブルを記憶する手段と、

前記ホームネットワークの外部に位置する第 1 の通信装置から、前記第 2 のアクセス番号の使用により、前記所定のメッセージを受信する手段と、

使用された前記第 2 のアクセス番号から前記認証テーブルを参照して得られる認証方法に従って、前記第 1 の通信装置との間で認証手続きを行う手段と、

前記認証に成功した場合に、使用された前記第 2 のアクセス番号から前記認証テーブルを参照して得られる前記第 1 のアクセス番号を使用し、所定のアクセス網を介して、前記ホームゲートウェイ装置へ、前記所定のメッセージを送信する手段とを備えたことを特徴とするアクセスサーバ装置。

【請求項 5】前記所定のメッセージを前記ホームゲートウェイ装置に転送した後に該ホームゲートウェイ装置から情報を受信する手段と、

受信した該情報を、前記第 1 の通信装置に転送するために、前記第 1 の通信装置へ送信する手段とを更に備えたことを特徴とする請求項 4 に記載のアクセスサーバ装置。

【請求項 6】前記情報は、前記ホームゲートウェイ装置により作成された、該ホームゲートウェイ装置の設置されたホームネットワーク上に接続されている機器に関する内容を含むホームページであることを特徴とする請求項 5 に記載のアクセスサーバ装置。

【請求項 7】前記情報は、前記所定のメッセージを転送した前記第 2 の通信装置から送信され、該ホームゲートウェイ装置によりプロトコル変換された、所定の形式のデータであることを特徴とする請求項 5 に記載のアクセスサーバ装置。

【請求項 8】前記ホームゲートウェイ装置との間の通信を、暗号処理または改ざん防止処理を施した上で行なうことを特徴とする請求項 4 のアクセスサーバ装置。

【請求項 9】前記認証テーブルに、複数のホームゲートウェイ装置を登録可能としたことを特徴とする請求項 4 のアクセスサーバ装置。

【請求項 10】前記アクセスサーバ装置は、前記アクセス網を提供する通信事業者によって提供されるものであることを特徴とする請求項 4 ないし 9 に記載のアクセスサーバ装置。

【請求項 11】前記第 1 の通信装置は、インターネット

を介して、前記アクセスサーバ装置へアクセスすることを特徴とする請求項 4 ないし 10 に記載のアクセスサーバ装置。

【請求項 12】前記アクセスサーバ装置へ専用線を介してアクセスすることを特徴とする請求項 4 ないし 11 に記載のアクセスサーバ装置。

【請求項 13】ホームネットワークに接続可能な家電機器に関して制御画面を含むデータを登録したデータベースを記憶する手段と、  
前記ホームゲートウェイ装置から未知の家電機器に関する問い合わせメッセージを受信する手段と、  
問い合わせを受けた前記家電機器のデータについて前記データベースを検索する手段と、  
前記検索の結果得られたデータを含む応答メッセージを、問い合わせもとの前記ホームゲートウェイ装置に送信する手段とを更に備えたことを特徴とする請求項 4 ないし 12 に記載のアクセスサーバ装置。

【請求項 14】前記認証テーブルに登録された前記ホームゲートウェイに対して、該ホームゲートウェイの設置されたホームネットワークから外部への方向のアクセスに対して、プロキシサーバ処理を代行して行うための手段を更に備えたことを特徴とする請求項 4 ないし 13 に記載のアクセスサーバ装置。

【請求項 15】前記ホームゲートウェイ装置は、自装置が設置されたホームネットワークの外部からのアクセスについては、予め登録された前記アクセスサーバ装置からのアクセスのみを許可するものであることを特徴とする請求項 4 ないし 14 に記載のアクセスサーバ装置。

【請求項 16】ホームネットワークに設置されるホームゲートウェイ装置であって、  
前記ホームネットワークと所定のアクセス網との間を中継するための手段と、  
前記所定のアクセス網を介して通信可能な、自装置に対するアクセス制御を依頼しているアクセスサーバ装置を登録するための手段と、  
自装置が設置されたホームネットワークの外部からのアクセスを受けた際に、予め登録された前記アクセスサーバ装置からのアクセスのみを許可する手段とを備えたことを特徴とするホームゲートウェイ装置。

【請求項 17】前記アクセスが許可された場合に、前記アクセスサーバ装置から受信した所定のメッセージを、自装置の接続されたホームネットワークのプロトコルにプロトコル変換した上で、該ホームネットワーク上の宛先通信装置に転送する手段を更に備えたことを特徴とする請求項 16 に記載のホームゲートウェイ装置。

【請求項 18】前記宛先通信装置に前記所定のメッセージを転送した後に該宛先通信装置から受信した所定の形式の AV データを、前記アクセスサーバに中継する手段と、  
受信した前記所定の形式の AV データに対して所定の変

換処理を施す手段とを更に備えたことを特徴とする請求項 17 に記載のホームゲートウェイ装置。

【請求項 19】前記アクセスが許可された場合に、前記アクセスサーバ装置から受信した所定のメッセージに回答して、自装置の接続されたホームネットワーク上に接続されている機器に関する内容を含むホームページを返送する手段を更に備えたことを特徴とする請求項 16 に記載のホームゲートウェイ装置。

【請求項 20】自装置の設置されたホームネットワークについて自動構成認識を行う手段と、  
前記自動構成認識において、前記ホームネットワーク上に、予め登録されていない未知の種類の機器又はサービスが検出された場合に、該未知の機器又はサービスに関する問い合わせメッセージを前記アクセスサーバ装置に送信する手段と、  
前記アクセスサーバ装置から、問い合わせた前記未知の機器又はサービスに関するデータを含む応答メッセージを受信する手段とを更に備えたことを特徴とする問い合わせることを特徴とする請求項 16 に記載のホームゲートウェイ装置。

【請求項 21】前記アクセスサーバ装置との間の通信を、暗号処理または改ざん防止処理を施した上で行なうことを特徴とする請求項 16 ないし 20 のいずれか 1 項に記載のホームゲートウェイ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ホームネットワークに設置されるホームゲートウェイ装置、ホームゲートウェイ装置へのアクセスを制御するアクセスサーバ装置及び通信方法に関する。

【0002】

【従来の技術】デジタル家電の急速な普及に伴い、家電機器同士をネットワーク接続するいわゆる「ホームネットワーク」が急速に普及しようとしている。これは、AV 機器に代表される IEEE 1394、白物家電に代表されるエコネット、パソコンや周辺機器に代表されるイーサネット（登録商標）や USB 等、分野を問わない現象である。

【0003】これらのホームネットワークをインターネットと接続し、家電製品にインターネット接続機能を持たせたり、インターネットから家電機器の制御を行なうことを可能としようとする動きが活発である。このために必要な装置が、ホームネットワークと公衆網（インターネット）との間に位置し、ホームネットワークへの入口ノードともいうべき「ホームゲートウェイ」である。ホームゲートウェイは、ホームルータの機能の他、インターネットプロトコルを理解しない機器がホームネットワーク上に多く存在することが考えられることから、プロトコル変換機能（いわゆるゲートウェイ機能）が備わっているのが一般的である。

【0004】このような装置の登場により、インターネットからホームネットワーク上の装置の遠隔制御等が可能になると考えられる。

【0005】

【発明が解決しようとする課題】この場合、問題になると考えられるのがセキュリティの問題である。すなわち、インターネット上には悪意ユーザ（例えば、特定または不特定の通信機器あるいはネットワークなどに対して不正あるいは違法の通信行為等を働こうとするあるいはその可能性のあるユーザ）が数多く存在することを前提とする必要があり、これらの悪意ユーザからのアタックを想定する必要がある。

【0006】企業ネットワークの場合には、企業ネットワークの入口ノードに「ファイアウォール」を配置し、ここで悪意ユーザからのアタックをシャットアウトするような方法が一般的であった。ところが、このような方法は、企業ネットワークに「ネットワーク管理者」を担当する者が存在し、該担当者が、セキュリティに関する適切な設定や、日々更新される「パッチあて」の作業等、セキュリティに関する管理業務を行なっていることが、暗黙の了解となっている。

【0007】これに対して、ホームネットワークの場合には、各一般家庭に、ホームゲートウェイへのセキュリティに関する適切な設定を行なうことのできるネットワーク管理者の存在を要求することはできない。したがって、ホームネットワークでは、ネットワーク管理者の存在を要求できる企業ネットワークのようにファイアウォール等によって悪意ユーザからの攻撃を防ぐというような技術を一般的に用いることはできない。

【0008】本発明は、上記事情を考慮してなされたもので、ホームゲートウェイに過度なセキュリティ機能を実装したり、ホームゲートウェイのユーザに専門的な設定、管理などを要求したりすることなしに、ホームネットワークに対する悪意ユーザからの攻撃を未然に防ぐことを可能とするホームゲートウェイ装置、アクセスサーバ装置及び通信方法を提供することを目的とする。

【0009】

【課題を解決するための手段】本発明に係る通信方法は、ホームネットワークの外部に位置する第1の通信装置から該ホームネットワーク上の第2の通信装置にアクセスするために、該第1の通信装置から、該ホームネットワークに設置されたホームゲートウェイ装置に対応するアクセス番号を指定して、該ホームゲートウェイ装置に対応するアクセスサーバ装置へ、所定のメッセージを送信し、前記所定のメッセージを受信した前記アクセスサーバ装置は、前記第1の通信装置との間で、該第1の通信装置について、予め定められた認証方法に従って認証手続きを行い、前記アクセスサーバ装置は、前記認証に成功した場合に、指定された前記アクセス番号に対応するホームネットワークに設置されたホームゲートウェイ

装置へ、所定のアクセス網を介して、該所定のメッセージを転送し、予め登録された前記アクセスサーバ装置から前記所定のメッセージを受信した前記ホームゲートウェイ装置は、該所定のメッセージを、前記第2の通信装置がサポートするプロトコルに変換した上で、該ホームネットワークを介して、前記第2の通信装置へ転送することを特徴とする。

【0010】また、本発明に係る通信方法は、ホームネットワークの外部に位置する通信装置から該ホームネットワークにアクセスするために、該通信装置から、該ホームネットワークに設置されたホームゲートウェイ装置に対応するアクセス番号を指定して、該ホームゲートウェイ装置に対応するアクセスサーバ装置へ、所定のメッセージを送信し、前記所定のメッセージを受信した前記アクセスサーバ装置は、前記通信装置との間で、該通信装置について、予め定められた認証方法に従って認証手続きを行い、前記アクセスサーバ装置は、前記認証に成功した場合に、指定された前記アクセス番号に対応するホームネットワークに設置されたホームゲートウェイ装置へ、所定のアクセス網を介して、該所定のメッセージを転送し、予め登録された前記アクセスサーバ装置から前記所定のメッセージを受信した前記ホームゲートウェイ装置は、該所定のメッセージに基づいて選択された該ホームネットワークに係る情報を含むホームページを、前記アクセスサーバ装置を経由して、前記通信装置に転送することを特徴とする。

【0011】また、本発明は、登録されたホームネットワークのホームゲートウェイ装置に対するアクセス制御を行うアクセスサーバ装置であって、自装置がアクセス制御を行う対象とする前記ホームゲートウェイ装置にアクセスするために使用すべき第1のアクセス番号と、該ホームゲートウェイ装置の設置されるホームネットワークの外部に位置する第1の通信装置が該ホームゲートウェイ装置または該ホームネットワーク上の第2の通信装置に所定のメッセージを送信する際に自装置へアクセスするために使用すべき第2のアクセス番号と、自装置が該第1の通信装置との間で行うべき認証方法とを対応付けて登録した認証テーブルを記憶する手段と、前記ホームネットワークの外部に位置する第1の通信装置から、前記第2のアクセス番号の使用により、前記所定のメッセージを受信する手段と、使用された前記第2のアクセス番号から前記認証テーブルを参照して得られる認証方法に従って、前記第1の通信装置との間で認証手続きを行う手段と、前記認証に成功した場合に、使用された前記第2のアクセス番号から前記認証テーブルを参照して得られる前記第1のアクセス番号を使用し、所定のアクセス網を介して、前記ホームゲートウェイ装置へ、前記所定のメッセージを送信する手段とを備えたことを特徴とする。

【0012】また、本発明は、ホームネットワークに設

置されるホームゲートウェイ装置であって、前記ホームネットワークと所定のアクセス網との間を中継するための手段と、前記所定のアクセス網を介して通信可能な、自装置に対するアクセス制御を依頼しているアクセスサーバ装置を登録するための手段と、自装置が設置されたホームネットワークの外部からのアクセスを受けた際に、予め登録された前記アクセスサーバ装置からのアクセスのみを許可する手段とを備えたことを特徴とする。

【0013】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【0014】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0015】本発明によれば、通信事業者等のサービス事業者側のアクセスサーバ装置にホームネットワーク側のセキュリティ機能（ファイアウォール機能）を受け持たせることで、ホームネットワーク側のホームゲートウェイ装置に過度なセキュリティ機能を実装したり、ホームゲートウェイ装置のユーザに専門的な設定、管理などを要求したりすることなしに、ホームネットワークに対する悪意ユーザからの攻撃を未然に防ぐことが可能になる。

【0016】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【0017】図1に、本実施形態の通信システムの全体構成例を示す。

【0018】図1に示されるように、家庭内のホームネットワーク1に、ホームゲートウェイ2と、家電やAVやPC等の各種デジタル家電機器（図1の例では、照明器具11とVTR12を例示している）が接続される。ホームネットワーク1は、例えばIEEE1394やエコーネット等のように、実際には複数のネットワーク技術から構成されていてもよい。また、ホームネットワーク1に接続された機器は、必ずしもインターネットプロトコルに準拠している必要はない。

【0019】ホームゲートウェイ1は、アクセス網3と接続される。アクセス網3は、例えば、携帯電話のネットワークである。アクセス網3にはアクセスサーバ4が接続されており、アクセスサーバ4がインターネット5と接続されている。

【0020】なお、アクセス網3上およびまたはホームネットワーク1上をインターネットプロトコル（IP）に準拠したプロトコルで動作させてもよい（ここでは、説明上、「アクセス網」と「インターネット」とを分け

て記述しているが、アクセス網がインターネットプロトコル（IP）に準拠したプロトコルで動作される場合を排除するものではない）。

【0021】アクセス網3やアクセスサーバ4はどのようなサービス事業者の管理に属するかについては、種々のバリエーションがある。例えば、アクセス網3とアクセスサーバ4の両方が、携帯電話等の通信事業者の管理に属する（この場合、通信事業者は、ISPサービスも提供していることになる）。また、例えば、アクセス網3が携帯電話等の通信事業者の管理に属し、アクセスサーバ4がISP事業者の管理に属する。また、その他の形態も可能である。

【0022】ホームゲートウェイ2は、ホームネットワーク1とアクセス網3との間をつなぐ装置である。ホームゲートウェイ2は、家庭内のホームネットワーク1に接続された各種機器（例えば、照明11やVTR12）を家庭外から制御したり、家庭内のAVコンテンツ（例えば、VTR12に録画されたAVコンテンツ）をアクセス網3を通して家庭外に送信したり、といった種々の機能を実現する。

【0023】なお、ホームネットワーク1の外部にいる装置（例えば、インターネット5に接続された装置）とホームネットワーク1上の装置とが通信を行う際に、少なくとも、ホームネットワーク1の外部にいる装置とホームゲートウェイ2との間、ホームネットワーク1の外部にいる装置とアクセスサーバ4との間、アクセスサーバ4とホームゲートウェイ2との間のいずれかにおいて、パケット通信を、暗号化や電子署名などを施して行うと好ましい。

【0024】図2に、ホームゲートウェイ2の内部構成例を示す。

【0025】図2に示されるように、ホームゲートウェイ2は、ホームネットワーク・インタフェース（ホームネットワークI/F）21、ホームネット自動構成認識部22、ホームネット制御ページ作成部23、ホームネット制御ページ送信部24、アクセスサーバプロトコル処理部25、アクセス網インタフェース（アクセス網I/F）26、プロトコル変換及びホームネット制御部27、高速AV/MPEG4変換部28を備えている。

【0026】本ホームゲートウェイ2では、ホームネットワークI/F21を介して接続されているホームネット自動構成認識部22が、ホームネットワーク1に接続された機器を自動的に検出する。例えば、ホームネットワーク1がIEEE1394であれば、IEEE1212レジスタの読み込みや、AV/Cコマンドの発行、HAViレジストリ処理等によって、自動構成認識を行なう。

【0027】この自動構成認識の結果を、「ホームページ」の形で制御画面に変換するのが、ホームネット制御ページ作成部23である。この「ホームページ」には、

例えば図3に示すような形で、ホームネットワーク1に接続された家電機器の制御ページが生成される。

【0028】この「ホームページ」の作成は自動的に行われる。このために、例えば、ホームネット制御ページ作成部23内に各機器に関するひな形の制御画面をあらかじめ有し、自動構成認識の結果を反映して、このひな形画面を組み合わせたか、各機器から送られてくる制御画面を組み合わせる等して、この「ホームページ」を作成すればよい。

【0029】生成された家電制御のためのホームページを、インターネット5側からの要求に従って送出するのが、ホームネット制御ページ送信部24である。ホームネット制御ページ送信部24は、アクセス網1/F3を経由して到着した、ホームゲートウェイ2に対するホームネット制御画面の送出要求メッセージを、アクセスサーバプロトコル処理部25にて判別し、当該要求をしたインターネット5側の装置(図示せず)に対して、ホームネット制御ページを送出する。

【0030】上記インターネット5側の装置は、この制御画面を通して、ホームネットワーク1に接続された家電機器の制御要求を行なう。該装置からの制御要求メッセージを受信して、具体的な制御を処理するのが、プロトコル変換及びホームネット制御部27である。プロトコル変換及びホームネット制御部27は、この制御要求メッセージを、ホームネットワーク1のプロトコルコマンド(例えばIEEE1394に接続された装置に対するAV機器への制御要求であれば、AV/Cコマンド)に変換して、これをホームネットワーク1/F21を通して該当機器に送信する。

【0031】例えば、この要求がホームネットワーク1に接続されたAV機器(例えば、VTR12)に対する「AVデータ再生」要求であったとすると、ホームゲートウェイ2は、該AV機器からAVデータを受信し、該AVデータを(ホームネットワーク1と比較して送信帯域等に制限がある)アクセス網3に適合させるための符号変換処理(例えば、MPEG2からMPEG4への変換処理)を、高速AV/MPEG4変換部28にて行なう。アクセス網1/F3を経由して、アクセス網3/インターネット5に対して送出する。

【0032】図4に、アクセスサーバ4の内部構成例を示す。

【0033】図4に示されるように、アクセスサーバ4は、アクセス網インタフェース(アクセス網1/F)31、ホームゲートウェイプロトコル処理部32、第1のファイアウォール処理部(ファイアウォール処理部A)33、ホームゲートウェイ制御ページ送信部34、インターネット・インタフェース(インターネット1/F)35、第2のファイアウォール処理部(ファイアウォール処理部B)36を備えている。なお、後述するように、家電機器データベース37を備えてもよい。

【0034】なお、本実施形態では、ファイアウォール処理部AはHTTPを処理する機能を含み、ファイアウォール処理部BはAVデータ転送のためのプロトコルを処理する機能を含むものとする。なお、その代わりに、例えば、ファイアウォール処理部Aはインターネット5からアクセス網3/ホームネットワーク1方向へのパケットを処理する機能を含み、ファイアウォール処理部Bはホームネットワーク1/アクセス網3からインターネット5方向へのパケットを処理する機能を含むように構成するなど、種々の方法がある。もちろん、ファイアウォール処理部を二つに分けずに構成してもよい。

【0035】アクセスサーバ4のインターネット5側には、ホームゲートウェイ制御ページ送信部34があり、ホームゲートウェイ制御ページ送信部34が、実際の(特定の)ホームゲートウェイ2のために、(該特定の)ホームゲートウェイの制御ページの送信を代行する。また、アクセス網3側には、ホームゲートウェイプロトコル処理部32があり、ホームゲートウェイ2とアクセスサーバ4との間に定義された後述するようなプロトコル処理を行なう。

【0036】なお、このアクセスサーバ4は、同時に複数のホームゲートウェイに対してサービスを提供することが可能であり、後述するようなサービスを、並行して、同時にいくつも提供することが可能である(すなわち、同時に複数のホームゲートウェイのプロキシとなることができる)。

【0037】次に、例えばユーザがこのホームゲートウェイを購入した際などに、ユーザが、このホームゲートウェイに対するプロキシサービスの利用を、該サービスを提供するサービス事業者(例えば、携帯電話等の通信事業者)へ申し込む場合について説明する。

【0038】本実施形態の場合、ホームゲートウェイ2に対するプロキシサービスの利用をサービス事業者に対して登録する。サービス事業者は、アクセスサーバ4を用意する。そのユーザ自身を含めた一般ユーザは、このアクセスサーバ4を介して、このホームゲートウェイ2にアクセスするようなアーキテクチャとなる(すなわち、アクセスサーバ4が、このホームゲートウェイ2のプロキシとなる)。これは、そのホームゲートウェイ2へのアクセスを、一旦、そのサービス事業者のアクセスサーバ4を経由させることで、いわゆる「ファイアウォール処理」等のセキュリティ機能をサービス事業者側によって提供することとし、ホームゲートウェイ4側に、過度なセキュリティ機能を用意しなくとも、ハッカーなどの悪意ユーザの進入防止に代表されるようなセキュリティ処理を達成させることが可能となる。

【0039】図5に、この場合のシーケンスの一例を示す。

【0040】まず、ユーザは、ホームゲートウェイ購入時あるいはそのホームゲートウェイの使用をサービス事

業者に申告（申し込み）するときなどの所定のタイミングで、そのユーザを認証するための認証方法（アクセスサーバとそのユーザとの間を認証するための認証方法）を登録する（ステップS1）。例えば、この個人認証方法としては、パスワードによる認証や、指紋照合や角膜照合、予め決められた鍵や署名の交換、特定の携帯電話やパソコンからのアクセスに限定してそのソースアドレス（電話番号等）から判定する方法等、種々のものが考えられる。

【0041】次に、サービス事業者は、そのユーザへ、そのホームゲートウェイ2に対するアクセスのために使用するべきアクセス番号を与える（ステップS2）。例えば、そのユーザが、自分のホームゲートウェイ2へのアクセスを携帯電話から行なうことを希望したとすると、サービス事業者は、そのホームゲートウェイ2に対するアクセスのために使用するべきアクセス番号として、例えば、090-1234-XXXXを与える。以降、ユーザは、このアクセス番号090-1234-XXXXを入力すれば、このホームゲートウェイ2へのアクセスを試みる事が可能となる（まず認証から行なうことになる）。

【0042】なお、ステップS1やS2での情報のやり取りは、アクセス網3を介して行ってもよいし、アクセス網3以外の通信網を介して行ってもよいし、記録媒体を介して行ってもよい。

【0043】さて、上記のように申告された内容が、アクセスサーバ4内のファイアウォール処理部A内の認証テーブルに登録される（ステップS3）。

【0044】ここで、認証テーブルの例を図6に示す。図6に例示されるように、この認証テーブルは、アクセス番号、個人認証方式、アクセス番号との通信方法、認証内容、プロキシサービスの対象となる実際のホームゲートウェイのアドレス（アクセス番号）などが記載されている。

【0045】この認証テーブルを参照することによって、

- ・どのアクセス番号にアクセスしてきたユーザについては、該ユーザが申し込みをした（あるいは予め登録された）本人であるかを、どのような個人認証方式で認証するか、およびその具体的な認証の手続きに関する認証内容、
- ・インターネット5側のユーザと、このアクセスサーバ4のアクセス番号との通信方法、
- ・プロキシサービスの対象となる実際のホームゲートウェイ2へのアクセスはどのように行なえばよいか、等を知ることができる。

【0046】なお、インターネット5側のユーザとこのアクセスサーバ4のアクセス番号との通信方法には、SSL、S-HTML等のセキュリティを確保するためのプロトコルを使用するのが好ましい。パケット通信を暗

号化や電子署名などを施して行うことによって、ユーザとアクセスサーバ4との間の通信の秘密を保つことが可能となる。

【0047】また、ホームゲートウェイ2側には、このアクセスサーバ4がいわゆる「プロキシサーバ」として登録される（ステップS4）。これは、ユーザが手動で行なってもよいし、サービス事業者あるいは販売店舗などが代行して設定してもよいし、ICカードやメモリカードなどに記憶させて、後でユーザがこのカードをホームゲートウェイ2に装着するなどして登録する方法により行なう等、様々な方法が考えられる。

10

【0048】このホームゲートウェイ2は、インターネット5側からあるいはアクセス網3側からあるいはホームネットワーク1の外部からのアクセスについて、プロキシサーバとして登録されたアクセスサーバ4以外からのアクセスは一切受け付けないようにする。このようにすることで、ホームゲートウェイ2のセキュリティの設定は著しく簡単なものとなる。また、このホームゲートウェイ2とアクセスサーバ4との間の通信は、例えばIPSec等のセキュリティプロトコルによって、成りすまし等の攻撃を未然に防ぐように設定される。または、アクセスサーバ4とホームゲートウェイ2との間は、専用線接続にて接続する。このようにすることで、ホームゲートウェイ2へのアクセスは、すべて（該ホームゲートウェイ2のプロキシとなっている）アクセスサーバ4を経由して行なわなければならないようになるため、該アクセスサーバ4のセキュリティが万全であれば、ホームゲートウェイ2あるいはホームネットワーク1に対する悪意ユーザからの進入等を未然に防ぐことが可能となる。

20

30

【0049】次に、インターネット5上の装置がアクセスサーバ4／アクセス網3／ホームゲートウェイ2を介して、ホームネットワーク1上の家電機器と通信する際のシーケンスについて説明する。

【0050】ここでは、具体例として、インターネット5に接続された携帯電話（例えばインターネットサービス利用機能を有する携帯電話等）からホームゲートウェイ2を介して家電機器を遠隔操作する場合について説明する。

40

【0051】図7および図8に、この場合のシーケンスの一例を示す。

【0052】ホームゲートウェイ2は、所定のタイミングで、ホームネット自動構成認識部22により、ホームネットワーク1側に対して構成問合せメッセージを送信し（ステップS11）、家電機器やホームネット1上のディレクトリサーバ（図示せず）などからの構成応答メッセージを受信し（ステップS12）、該構成応答メッセージに基づいて図3に例示するようなホームネットの制御ページを作成する（ステップS13）。

50

【0053】なお、ステップS13において、予めホー

い家電機器が検出さ  
ビス、サブユニット  
では制御ページが作  
合にはホームゲー  
合わせることによ  
る情報を取得できる

シーケンスの一例を

4は、例えば、最新  
情報などの詳細情  
家電機器データペ  
もちろん、最新の家電  
または一部の家電機  
てもよい)。図11  
を示す。

2は、ステップS13  
2に登録されていない  
ームゲーウェイ1  
ない家電機器を示す  
サービスの種別、あ  
問い合わせメッセー  
る(ステップS10

ページを受信したアク  
機器(例えば、機器、  
)について家電機器デ  
ノブS102)。

サーバ4は、問い合わせ  
種別に、適切なデータ  
制御画面等)を含む応  
103)。

を受信したホームゲー  
器に関する詳細情報や  
ホームネット制御ペー  
105)。

ウェイ2は、取得した  
制御画面等のデータを、  
制御部27に追加登録  
ップS104)。

ワーク1上の家電機器  
、携帯電話(図示せず)か  
こ、アクセス要求メッセ  
送出する(ステップS  
められたアクセス番号  
XXX)に対してアク  
サーバ4に対してアク  
はない(むしろ、所望  
アクセスしようとして

【0062】アクセス要求メッセージを受けたアクセス  
サーバ4は、要求されたアクセス番号をもとに、認証テ  
ーブルを参照して、認証方式を確認し(ステップS2  
2)、これに合わせて送信ユーザ(携帯電話)に対して  
認証のチャレンジを行なう(ステップS23)。

【0063】この認証のチャレンジを受けた携帯電話  
は、適切なレスポンス(例えばパスワード入力や指紋の  
入力など)をアクセスサーバに返す(ステップS2  
4)。

【0064】このレスポンスを受けたアクセスサーバ4  
は、認証内容の確認を行なう(ステップS25)。

【0065】もし、本人であることの確認がなされたな  
らば、アクセスサーバ4は、認証テーブルを参照して該  
当するホームゲーウェイ2を調べ、該ホームゲートウ  
ェイ2に対して、アクセス網3を通して、初期ページの  
送信要求を行なう(ステップS26)。

【0066】送信要求メッセージを受けたホームゲー  
トウェイ2は、アクセス網3を通して、初期ページをアク  
セスサーバに送信する(ステップS27)。

【0067】なお、ステップS11～S13は、ステッ  
プS26とステップS27との間で行ってもよい。

【0068】アクセスサーバ4は、このようにして取得  
した初期ページを、自身のホームゲーウェイ制御ペー  
ジ送信部34が送信しているがごとく振るまい、携帯電  
話に対して、これを送信する(ステップS28)。な  
お、その際、アクセスサーバ4は、HTMLからC-H  
TML(コンパクトHTML;携帯電話で使われるWe  
bページの記述言語の一種)への変換など、必要なホー  
ムページの記述形式の変換を行なってもよい。また、ホ  
ームゲーウェイ2が持つ初期ページを予めキャッシュ  
しておいてもよい。

【0069】さて、ここで、携帯電話が「ホームネット  
制御ページ」の送信要求メッセージを送ってきたとする  
(ステップS29)。アクセスサーバ4のファイアウォ  
ール処理部Aは、このセキュリティ確認を行ない(ステ  
ップS30)、確認が取れた(予め登録されたユーザか  
らの要求であると確認された)場合、ホームネット制御  
ページ要求メッセージをホームゲーウェイ2に対して  
送信する(ステップS31)。

【0070】ホームゲーウェイ2は、ホームネット制  
御ページをアクセスサーバ4に対して送信する(ステッ  
プS32)。

【0071】この制御ページは、アクセスサーバ4のホ  
ームゲーウェイ制御ページ送信部34を介して、携帯  
電話に送られる(ステップS33)。なお、携帯電話  
は、アクセスサーバ4からこの制御ページが送られてき  
た、という認識を持っていてもよい。

【0072】ここで、携帯電話にて、例えば制御対象の  
装置としてVTRが指定されたとすると、その制御コマ  
ンド(例えばホームネット制御ページの適切なボタンを

押す動作)がアクセスサーバ4に伝えられる(ステップS34)。

【0073】アクセスサーバ4は、再びセキュリティの確認を行ない(ステップS35)、確認が取れた場合は、ホームゲートウェイ2に対して、VTR制御のためのコマンド(例えばホームネット制御ページの適切なボタンを押す動作)を送信する(ステップS36)。

【0074】ホームゲートウェイ2では、受け取ったコマンドをプロトコル変換及びホームネット制御部27においてホームネットワークプロトコルに準拠した制御コマンドに変換して(ステップS37)、これをVTRなどの家電機器に送信する(ステップS38、S39)。その際、必要な場合は、ホームネットワーク上での帯域確保等も伴うことがある。

【0075】さて、この結果、家電機器から例えば高速映像信号などがホームゲートウェイ2に対して流れてくる(ステップS40)。

【0076】ホームゲートウェイ2の高速AV/MPEG4変換部28は、この高速映像信号をMPEG4信号などに変換する(ステップS41)。このようにすることにより、アクセス網に適した形(例えば、限定された帯域に合わせて、映像の高圧縮が行なわれる)でデータ送信を行なうことができるようになる。

【0077】このように変換されたMPEG4映像は、アクセスサーバ4に対して送られる(ステップS42)。

【0078】アクセスサーバ4では、ファイアウォール処理部Bにおいて、必要なファイアウォール処理(NAT処理やIPマスカレード処理)を施し(ステップS43)、このMPEG4映像は、インターネット5を介して携帯電話に届けられる(ステップS44)。

【0079】このようにして、携帯電話のユーザは、携帯電話/インターネットを通して自宅の家電を制御したり、自宅内のAVコンテンツを携帯電話にて閲覧したりといったことが可能となる。

【0080】なお、上記では、携帯電話からアクセスサーバ4までの接続が一旦インターネット5を経由するものとして説明したが、例えばインターネットサービスを提供する通信事業者の通信網(図1のアクセス網3であってもよい)を経由して携帯電話がアクセスサーバ4に接続する(すなわちインターネット5を経由せずに接続する)ような場合も同様である。

【0081】これまでは、インターネット5側からホームネット1側へのアクセスについての例であった。次に、ホームネット1側からインターネット5側へのアクセスの例について説明する。

【0082】図9に、この場合のシーケンスの一例を示す。

【0083】ここでは、ホームネットワーク1上に家電機器としてパソコンが接続されたと仮定して(図示せ

ず)、このパソコンからインターネット5上のWWWサーバ(図示せず)へのアクセスが行なわれた場合を例にとって説明する。

【0084】まず、前述のようにパソコン上には、アクセスサーバ4がプロキシサーバとして登録されている(ステップS51)。

【0085】パソコン上からインターネット5上のWWWサーバへのアクセス要求があった場合、プロキシサーバであるアクセスサーバ4に対して、そのアクセス要求メッセージが送られる(ステップS52)。

【0086】アクセスサーバ4では、ファイアウォール処理部Aによってプロキシ処理が行なわれ(ステップS54)、実際のWWWサーバに対してアクセス要求メッセージが転送される。ただし、このアクセスサーバ4が要求したものとして転送される。

【0087】WWWサーバは、これに対する応答メッセージを送信し、これをアクセスサーバ4のファイアウォール処理部Aが受信する(ステップS55)。

【0088】アクセスサーバ4のファイアウォール処理部Aは、該応答メッセージについて、プロキシサーバ処理(例えばNATやIPマスカレード処理、アプリケーションゲートウェイ処理など)を行ない(ステップS56)、実際の応答メッセージをパソコンに転送する(ステップS57)。

【0089】このやり取りが、任意のWWWサーバに対するアクセスに対して行なわれる。

【0090】なお、図9上では、パソコンからアクセスサーバ4に対して直接パケットが飛んでいるように記述されているが、もちろんホームゲートウェイ2にて一旦パケットが終端されてもよい。すなわち、ホームゲートウェイ2において、アプリケーションゲートウェイ処理やNAT処理、IPマスカレード処理などの処理がなされて、アクセスサーバ4から見るとホームゲートウェイ2のみと通信しているように見えるようなアーキテクチャとなってもよい。

【0091】この場合は、パソコンに登録されているプロキシサーバがホームゲートウェイであってもよい。

【0092】また、上記では、WWWサーバはインターネット上に存在するものとして説明したが、例えばインターネットサービスを提供する通信事業者の通信網(図1のアクセス網3であってもよい)内に存在するWWWサーバにアクセスする(すなわちインターネット5を経由せずにアクセスする)ような場合も同様である。

【0093】また、サービス事業者によって提供される(アクセスサーバ4による)プロキシサービスを利用するか、ユーザが従来のようにネットワーク管理者になってホームゲートウェイ2に対して直接必要な設定や作業を行うかを、ユーザ自身が任意に選択できるようにしてもよい。また、それらを併用可能としてもよい。

【0094】なお、基本的にはアクセスサーバが提供す

るプロキシサービスを利用するものとした上で、さらにホームゲートウェイ 2 にネットワーク管理者に要求される知識を有さずとも簡易な手続きで認証のための設定ができる機能を付与し、限られた装置またはユーザのみ外部（インターネット）から直接ホームゲートウェイ 2 にアクセスできるようにしてもよい。例えば、ホームゲートウェイ 2 にパスワード等を登録しておき、外部からのアクセス時にユーザが正しいパスワード等を携帯電話等の端末装置へ入力し（あるいは携帯端末等にパスワード等を登録しておきあるいは登録されており）、正しいパスワード等を返答してきた携帯端末のみホームゲートウェイ 2 がアクセスを許可する方法など、種々の方法がある。

【0095】なお、以上の各機能は、ソフトウェアとしても実現可能である。また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【0096】なお、本実施形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。また、本実施形態内において、各種構成部分についての各種バリエーションは、適宜組み合わせることで実施することが可能である。また、各実施形態は、個別装置としての発明、関連を持つ 2 以上の装置についての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またばカテゴリに係る発明を包含・内在するものである。

【0097】従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されことなく発明を抽出することができるものである。

【0098】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0099】

【発明の効果】本発明によれば、通信事業者等のサービス事業者側のアクセスサーバ装置にホームネットワーク側のセキュリティ機能（ファイアウォール機能）を受け持たせることで、ホームネットワーク側のホームゲート

ウェイ装置に過度なセキュリティ機能を実装したり、ホームゲートウェイ装置のユーザに専門的な設定、管理などを要求したりすることなしに、ホームネットワークに対する悪意ユーザからの攻撃を未然に防ぐことが可能になる。

【図面の簡単な説明】

【図 1】本発明の一実施形態に係る通信システムの全体構成例を示す図

10 【図 2】同実施形態に係るホームゲートウェイの内部構成例を示す図

【図 3】同実施形態に家電機器の制御ページの一例を示す図

【図 4】同実施形態に係るアクセスサーバの内部構成例を示す図

【図 5】同実施形態に係る登録のためのシーケンスの一例を示す図

【図 6】同実施形態に係る認証テーブルの一例を示す図

【図 7】同実施形態に係る外部からホームネットワーク側へのアクセスの際のシーケンスの一例を示す図

20 【図 8】同実施形態に係る外部からホームネットワーク側へのアクセスの際のシーケンスの一例を示す図 7 の続きの図

【図 9】同実施形態に係るホームネットワーク側から外部へのアクセスの際のシーケンスの一例を示す図

【図 10】同実施形態に係るホームネット制御ページの際のシーケンスの一例を示す図

【図 11】同実施形態に係る家電機器データベースの一例を示す図

【符号の説明】

30 1…ホームネットワーク

2…ホームゲートウェイ

3…アクセス網

4…アクセスサーバ

5…インターネット

11…照明器具

12…VTR

21…ホームネットワーク・インタフェース

22…ホームネット自動構成認識部

23…ホームネット制御ページ作成部

40 24…ホームネット制御ページ送信部

25…アクセスサーバプロトコル処理部

26、31…アクセス網インタフェース

27…プロトコル変換及びホームネット制御部

28…高速AV/MPEG4変換部

32…ホームゲートウェイプロトコル処理部

33…第1のファイアウォール処理部

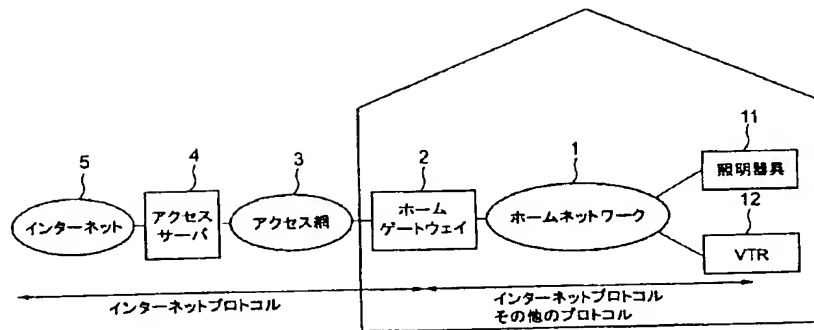
34…ホームゲートウェイ制御ページ送信部

35…インターネット・インタフェース

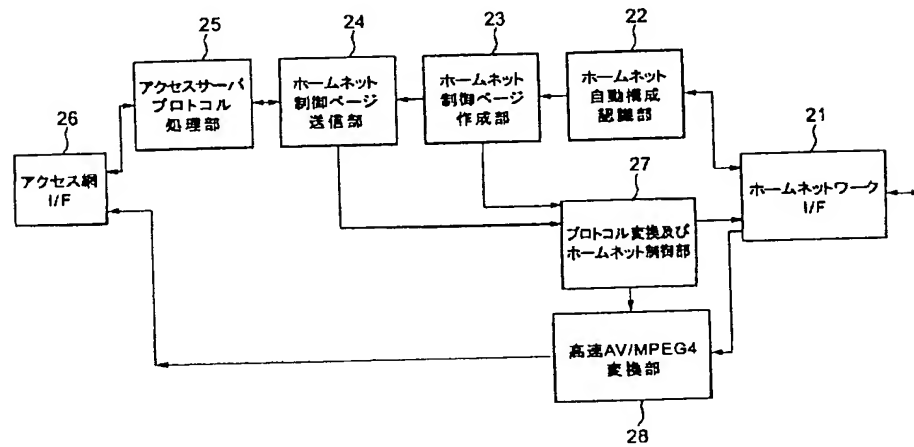
36…第2のファイアウォール処理部

50 37…家電機器データベース

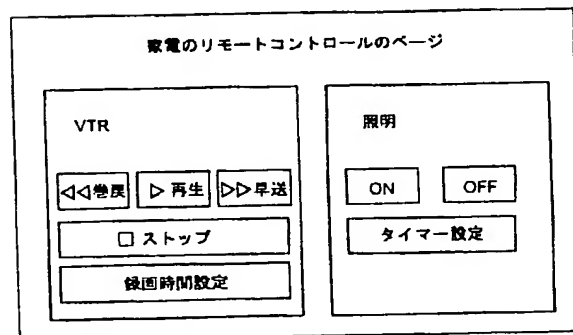
【図1】



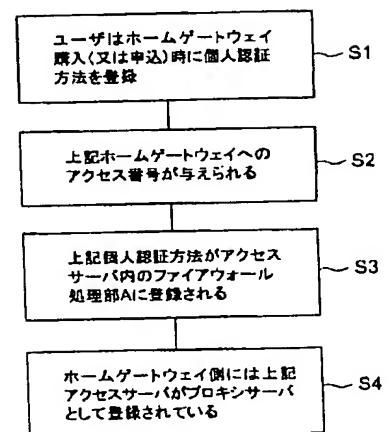
【図2】



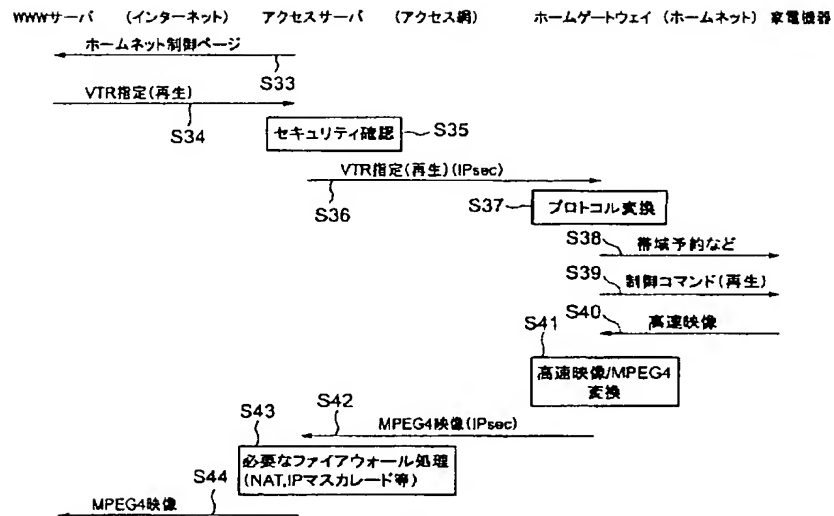
【図3】



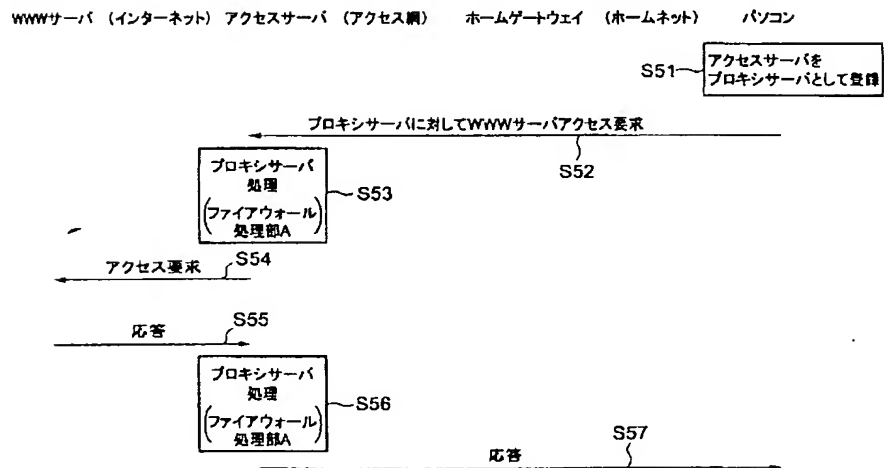
【図5】



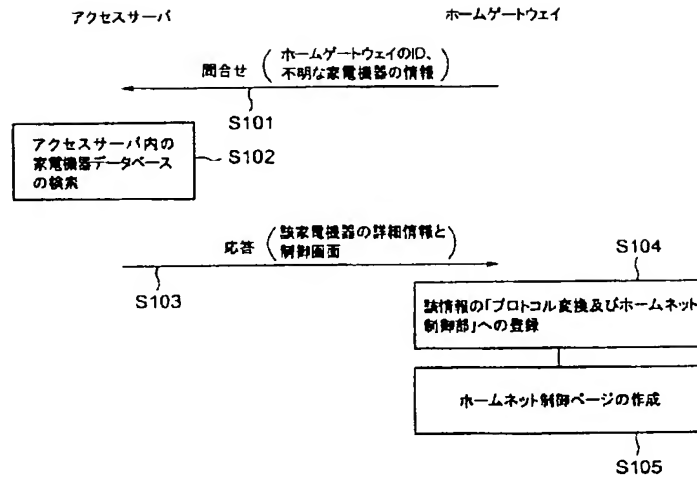
【図8】



【図9】



【図10】



【図11】

ネットワーク種別	サービス/サブユニット名	属性情報	制御画面
IEEE1394	ホームサーバ	(XMLデータ形式)	(XMLデータ形式)
⋮	⋮	⋮	⋮
エコーネット	自動そうじ機	(XMLデータ形式)	(XMLデータ形式)
⋮	⋮	⋮	⋮

(これらがホームゲートウェイの機種別に用意される)